Capital One | Cyber

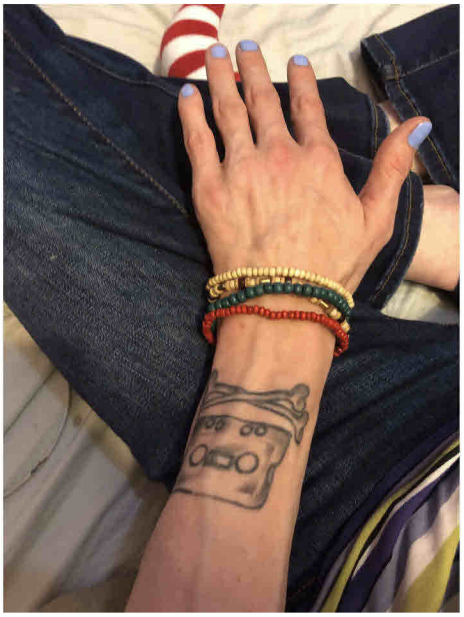
Law Enforcement Referral
July 20, 2019

Key Points

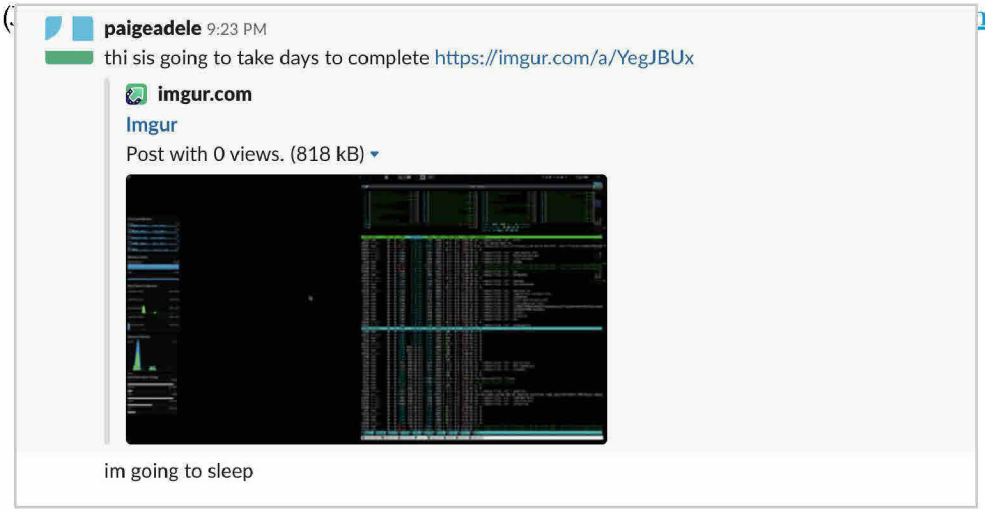
- On 17 July 2019, Capital One Financial was notified about a misconfiguration of its cloud infrastructure and a malicious actor has shared the results of exploiting this misconfiguration with many unidentified individuals on a Github data repository https://gist.github[.]com/paigeadelethompson/.
    - Capital One's investigations determined that the actor exploited the misconfiguration to steal data from Capital One's non-public data storage.
    - The Github data repository is linked to an individual by the name of Paige Adele Thompson. Based on the user identification (ID) and associated email of the repository, Capital One was able to determine the actor's identity, including other online IDs and emails, and observe public discussions admitting to the actions mentioned.
- On 19 July 2019, Capital One was able to determine that the reporter of the misconfiguration is not cooperating with the malicious actor. Capital One representative spoke directly with the reporter, facilitated through our responsible disclosure vendor, to obtain additional background on the situation and the actor. The reporter noted that Thompson is aware of the illegal nature of her actions and noted to others that people can "call the FBI on me."
- On 20 July 2019, Capital One learned of a Twitter post in which the actor stated an intention to share certain Capital One information she purportedly obtained.
- Capital One's review of online posts indicates that Thompson has an AWS scanning tool looking for open or easy to access instances, so she can illegally install a cryptocurrency mining software on identified instances. In the process, as she exploits these instances, she obtains permissions on these instances to be able to download data. (Appendix 2)
    - Thompson has professional experience at Amazon AWS, specifically as a Systems Engineer on S3, which includes automation and security. (Appendix 1)
    - Thompson claims to have victimized at least several additional companies. (Appendix 4)

Identified Actor

Name	Paige Adele Thompson *(Appendix 1)* (DOB: 1986) *Possible Alternative Name: Trevor A. Thompson* (DOB: 1986)
Title	CTO of Netcrave Communications
Email	Current email - erratic@yourstruly[.]sx, paigeadele@gmail[.]com, paige.adele.thompson@gmail[.]com Old email - erratic@devel[.]ws
Online Handles & Presence	https://twitter[.]com/erraticfake https://twitter[.]com/@0xA3A97B6C http://gitlab[.]com/netcrave https://gist.github[.]com/paigeadelethompson/ https://gist.github.com/paigeadelethompson/1d046e22a54995ebf82040d9279317cc https://gist.github.com/paigeadelethompson/9edf57dc3b10f72db5c8dc8e6ce16b9b https://gist.github.com/paigeadelethompson/b8cc49efffb2949857ccc60d3e3d8fa3 https://gist.github.com/paigeadelethompson/3bbb3f7fc187f83264455f51ce18525e https://twitter[.]com/paigethylamine {suspended} https://www.gitmemory[.]com/paigeadelethompson https://peegeepee.com/35A2274AAD8F627531F9A923581559E73563B9D1 paigeadele - Netcrave Slack
Reported Addresses	Current: 6520 28th Ave S, Seattle, Washington 98108 Old: 4343 NE Woodinville Duvall Rd, Woodinville, Washington 98072 Old: 226 Eastlake Ave E #80, Seattle, Washington 98109
Phone Number	206-946-2468

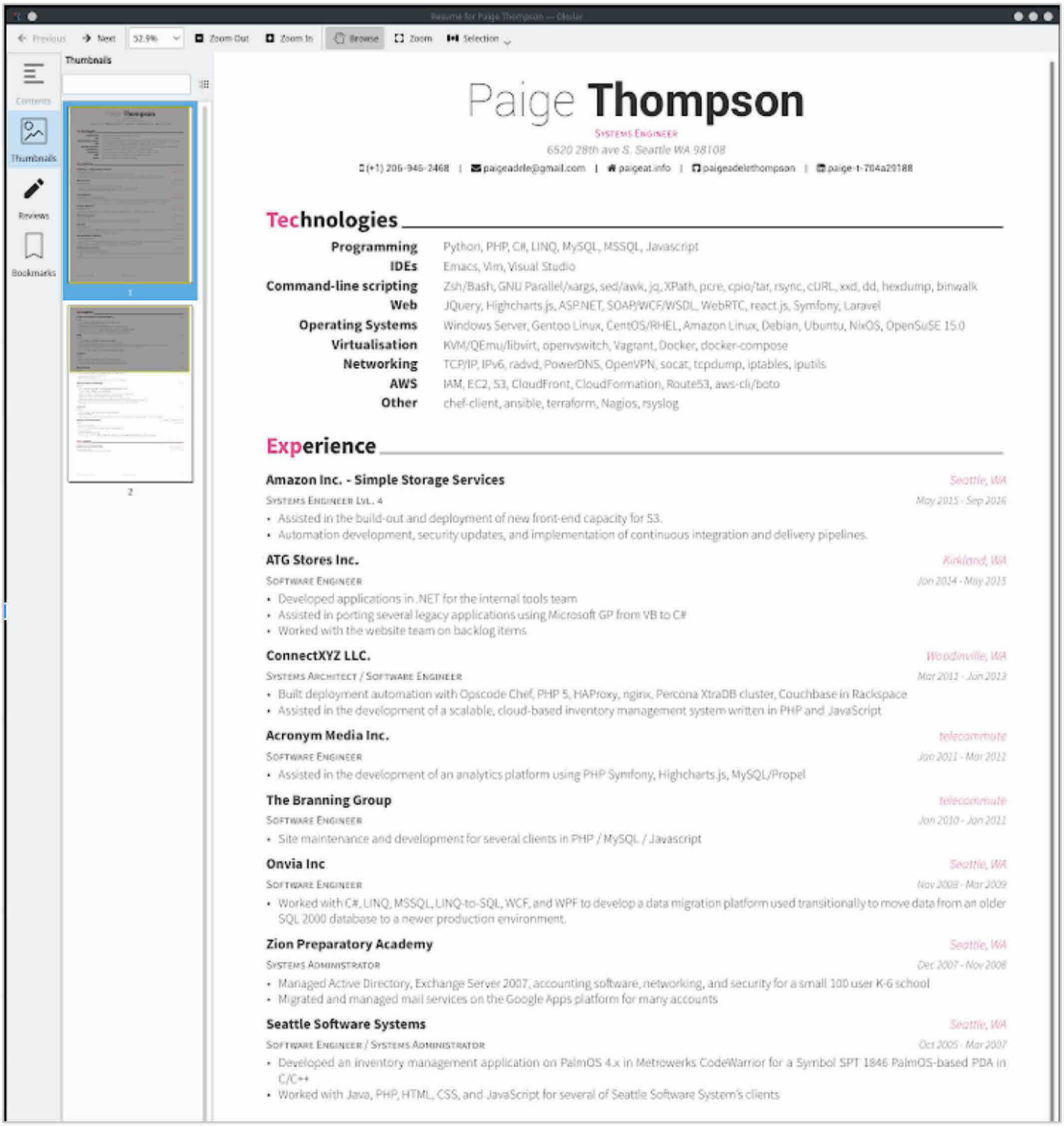


Observed Unauthorized Activities

Date	Activity Observed	Comments:
March 12, 2019 March 22, 2019 March 23, 2019	After an initial probe on March 12, a unauthorized user gained access to Capital One's AWS infrastructure by exploiting a misconfiguration on a web application firewall (WAF). The unauthorized actor was able to gain access to a server and enumerated the names of 746 S3 buckets on March 22 and March 23..	An unauthorized user exfiltrated 816.6GB of data from 229 of those buckets on March 22/23.
April 19, 2019 April 21, 2019 May 26, 2019	An unauthorized user made additional access attempts.	An unauthorized user unsuccessfully attempted to determine the privileges associated with the role by testing functions available (e.g. creating a key pair, describing the existing key pair).
June 26, 2019	The actor held discussions about Capital One ISRM WAF Role and data to other individuals.	Netcrave Slack is a place where hackers talk about various topics that include coding, devices, illegal activities, drug use, cryptocurrency mining, and others.
Screenshot (		n/a/YegJBUx
July 17, 2019	Capital One was notified about the possible proxy misconfiguration on a COF application hosted in AWS. The reporting party shared a 'secret' GitHub Gist containing proof of concept code which contained an enumerated list of S3 bucket names.	Investigations determined that successful exploitation enabled an authorized user to gain access to the server, including the ability to run commands and access the back-end AWS metadata service.

Appendix

1. June 26, 2019 - Screenshot of Resume from an IRC channel
- *Note: AWS - Simple Storage Service experience*



Paige Thompson

SYSTEMS ENGINEER

6520 28th ave S. Seattle WA 98108

(+1) 206-946-2468 | paigeadele@gmail.com | paigeat.info | paigeadelethompson | paige-t-704a29188

Technologies

Programming	Python, PHP, C#, LINQ, MySQL, MSSQL, Javascript
IDEs	Emacs, Vim, Visual Studio
Command-line scripting	Zsh/Bash, GNU Parallel/xargs, sed/awk, jq, XPath, pcre, cpio/tar, rsync, cURL, xxd, dd, hexdump, binwalk
Web	JQuery, Highcharts.js, ASP.NET, SOAP/WCF/WSDL, WebRTC, react.js, Symfony, Laravel
Operating Systems	Windows Server, Gentoo Linux, CentOS/RHEL, Amazon Linux, Debian, Ubuntu, NixOS, OpenSuSE 15.0
Virtualisation	KVM/QEmu/libvirt, openvswitch, Vagrant, Docker, docker-compose
Networking	TCP/IP, IPv6, radvd, PowerDNS, OpenVPN, socat, tcpdump, iptables, iputils
AWS	IAM, EC2, S3, CloudFront, CloudFormation, Route53, aws-cli/boto
Other	chef-client, ansible, terraform, Nagios, rsyslog

Experience

Amazon Inc. - Simple Storage Services — Seattle, WA

SYSTEMS ENGINEER LVL. 4 — May 2015 - Sep 2016

- Assisted in the build-out and deployment of new front-end capacity for S3.
- Automation development, security updates, and implementation of continuous integration and delivery pipelines.

ATG Stores Inc. — Kirkland, WA

SOFTWARE ENGINEER — Jan 2014 - May 2015

- Developed applications in .NET for the internal tools team
- Assisted in porting several legacy applications using Microsoft GP from VB to C#
- Worked with the website team on backlog items

ConnectXYZ LLC. — Woodinville, WA

SYSTEMS ARCHITECT / SOFTWARE ENGINEER — Mar 2013 - Jan 2013

- Built deployment automation with Opscode Chef, PHP 5, HAProxy, nginx, Percona XtraDB cluster, Couchbase in Rackspace
- Assisted in the development of a scalable, cloud-based inventory management system written in PHP and JavaScript

Acronym Media Inc. — telecommute

SOFTWARE ENGINEER — Jan 2011 - Mar 2012

- Assisted in the development of an analytics platform using PHP Symfony, Highcharts.js, MySQL/Propel

The Branning Group — telecommute

SOFTWARE ENGINEER — Jan 2010 - Jan 2011

- Site maintenance and development for several clients in PHP / MySQL / Javascript

Onvia Inc — Seattle, WA

SOFTWARE ENGINEER — Nov 2008 - Mar 2009

- Worked with C#, LINQ, MSSQL, LINQ-to-SQL, WCF, and WPF to develop a data migration platform used transitionally to move data from an older SQL 2000 database to a newer production environment.

Zion Preparatory Academy — Seattle, WA

SYSTEMS ADMINISTRATOR — Dec 2007 - Nov 2008

- Managed Active Directory, Exchange Server 2007, accounting software, networking, and security for a small 100 user K-6 school
- Migrated and managed mail services on the Google Apps platform for many accounts

Seattle Software Systems — Seattle, WA

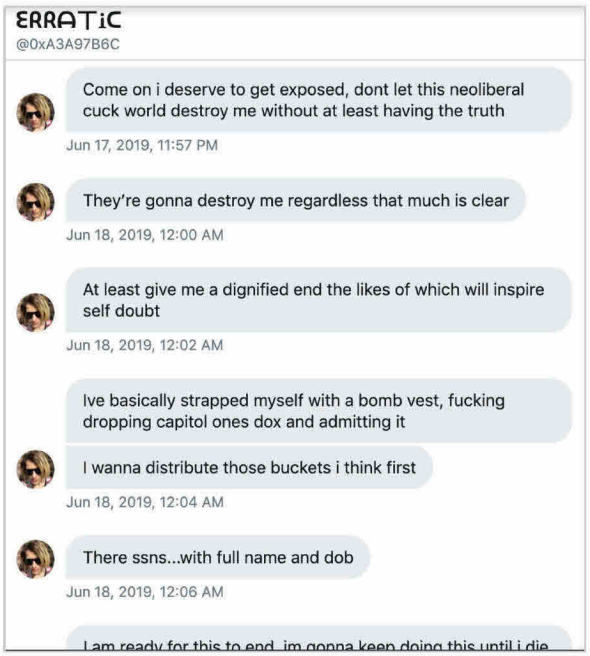
SOFTWARE ENGINEER / SYSTEMS ADMINISTRATOR — Oct 2005 - Mar 2007

- Developed an inventory management application on PalmOS 4.x in Metrowerks CodeWarrior for a Symbol SPT 1846 PalmOS-based PDA in C/C++
- Worked with Java, PHP, HTML, CSS, and JavaScript for several of Seattle Software System's clients

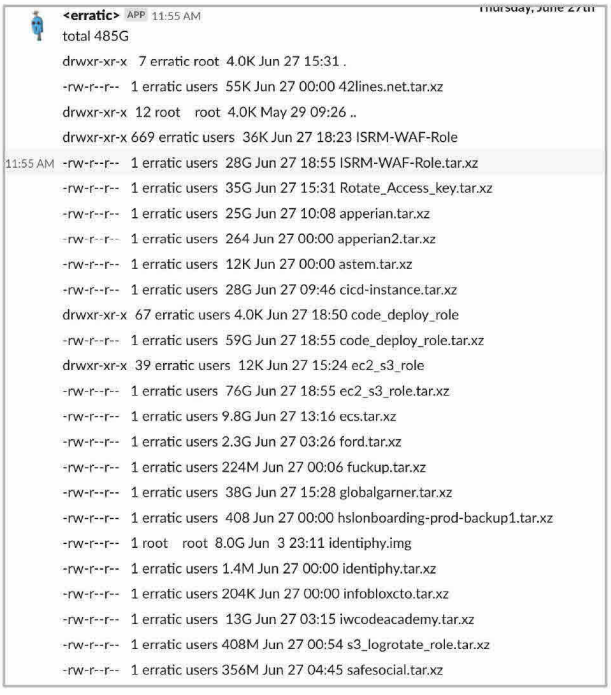
Appendix

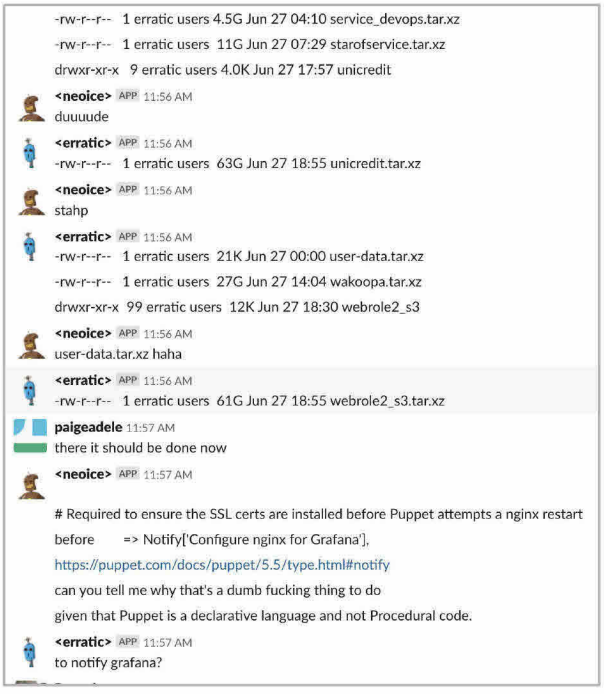
2. Actor's AWS Scanning/Mining Tool:
https://gist.github[.]com/paigeadelethompson/4555c7de22cc4e6749ad90ef976a54f9

3. Primary screenshot shared by reporter with Capital One on July 20, 2019.



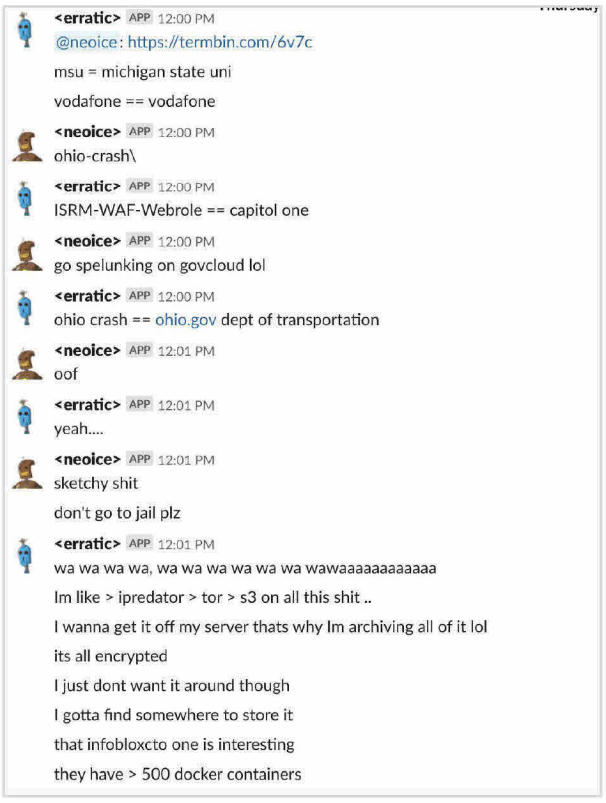
4. 26 June 2019, Screenshots showing Thompson downloaded data from other companies' data storage, including Capital One's ISRM-WAF-Role.

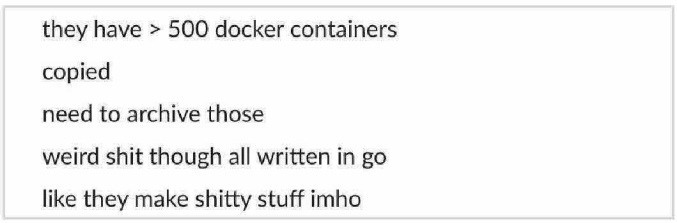




Appendix

4. Continued:





5. Full recording of screenshots shared by the reporter

ERRATIC
@0xA3A97B6C

Im gonna dox myself

Jun 17, 2019, 11:45 PM

gist:1d046e22a54995ebf82040d9279317cc
gist.github.com

Jacked gist.github.com/paigeadelethom... all avail s3 buckets, certs

Jun 17, 2019, 11:49 PM

ERRATIC
@0xA3A97B6C

Jacked gist.github.com/paigeadelethom... all avail s3 buckets, certs

Jun 17, 2019, 11:49 PM

gist:9edf57dc3b10f72db5c8dc8e6ce16b9b
gist.github.com

3tb of s3 buckets

Are we there yet

Jun 17, 2019, 11:52 PM

ERRATIC
@0xA3A97B6C

Are we there yet

Jun 17, 2019, 11:52 PM

gist:b8cc49efffb2949857ccc60d3e3d8fa3
gist.github.com

And im swatting other wizards botnets on mother fucking efnet

Jun 17, 2019, 11:56 PM

Come on i deserve to get exposed, dont let this neoliberal cuck world destroy me without at least having the truth

ERRATIC
@0xA3A97B6C

Come on i deserve to get exposed, dont let this neoliberal cuck world destroy me without at least having the truth

Jun 17, 2019, 11:57 PM

They're gonna destroy me regardless that much is clear

Jun 18, 2019, 12:00 AM

At least give me a dignified end the likes of which will inspire self doubt

Jun 18, 2019, 12:02 AM

Ive basically strapped myself with a bomb vest, fucking dropping capitol ones dox and admitting it

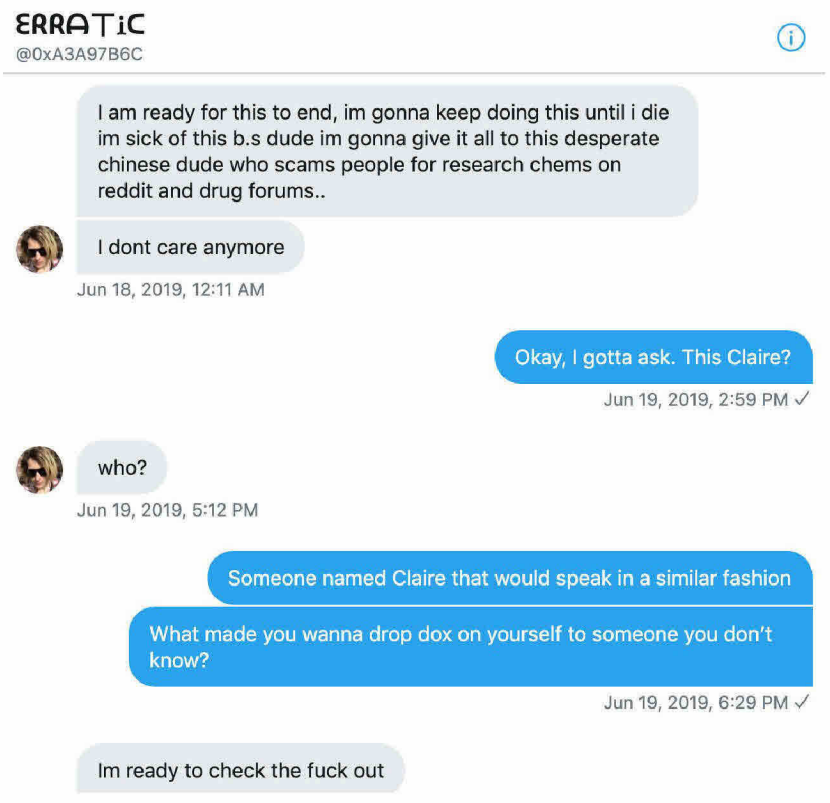
I wanna distribute those buckets i think first

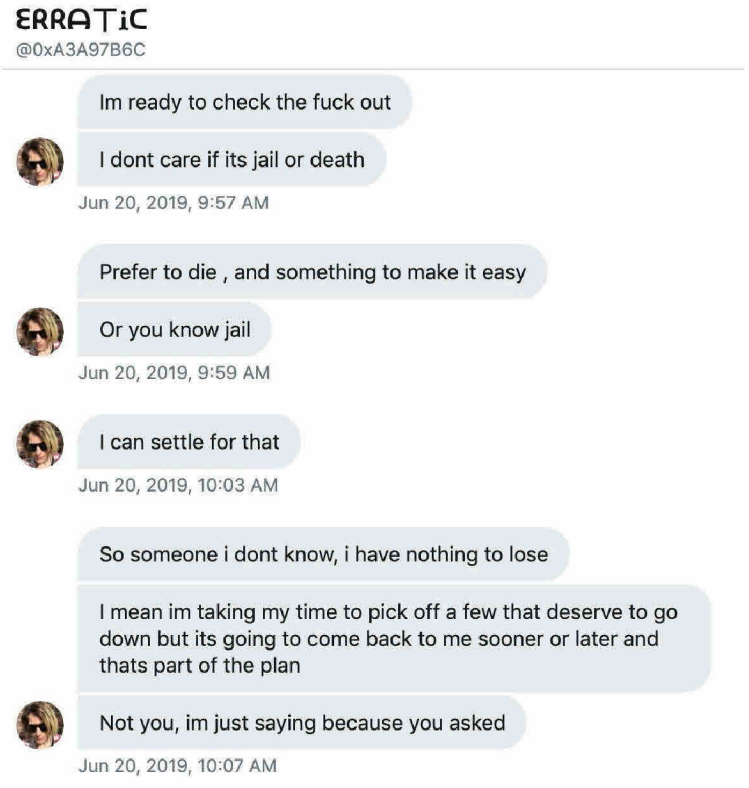
Jun 18, 2019, 12:04 AM

There ssns...with full name and dob

Jun 18, 2019, 12:06 AM

I am ready for this to end, im gonna keep doing this until i die


ERRATiC
@0xA3A97B6C
I am ready for this to end, im gonna keep doing this until i die im sick of this b.s dude im gonna give it all to this desperate chinese dude who scams people for research chems on reddit and drug forums..
I dont care anymore
Jun 18, 2019, 12:11 AM
Okay, I gotta ask. This Claire?
Jun 19, 2019, 2:59 PM ✓
who?
Jun 19, 2019, 5:12 PM
Someone named Claire that would speak in a similar fashion
What made you wanna drop dox on yourself to someone you don't know?
Jun 19, 2019, 6:29 PM ✓
Im ready to check the fuck out


ERRATiC
@0xA3A97B6C
Im ready to check the fuck out
I dont care if its jail or death
Jun 20, 2019, 9:57 AM
Prefer to die , and something to make it easy
Or you know jail
Jun 20, 2019, 9:59 AM
I can settle for that
Jun 20, 2019, 10:03 AM
So someone i dont know, i have nothing to lose
I mean im taking my time to pick off a few that deserve to go down but its going to come back to me sooner or later and thats part of the plan
Not you, im just saying because you asked
Jun 20, 2019, 10:07 AM

ERRATIC
@0xA3A97B6C

I spend most of my time baiting skids, using their names, collecting and using their dox and hacking shit my life was over 3 years ago

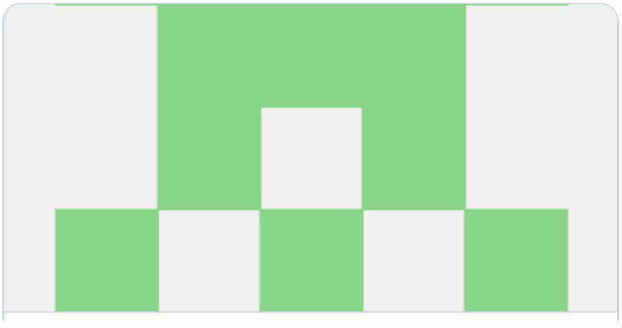
Almost 4

Gonna be 5

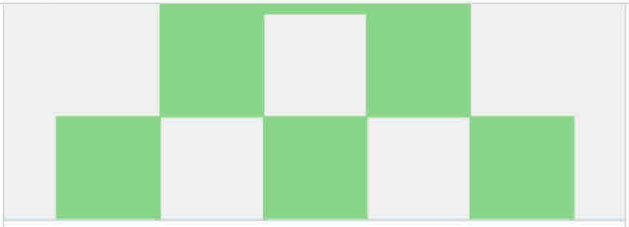
Im ok with that, it was my choice

I just need to be free

Jun 20, 2019, 10:10 AM



ERRATIC
@0xA3A97B6C



create s3 log bucket
gist.github.com

Go ahead and ddos my r5.large gist.github.com/paigeadelethom... while im asleep, i don't have to do anything the work is already done for me

Jun 20, 2019, 10:21 AM

Lam3r

Jun 21, 2019, 10:57 AM

Or not a snitch. Go snitch on yourself, fbi dot gov big homie

Jun 21, 2019, 10:59 AM ✓

You can no longer send messages to this person. Learn more